VIEW POINT

ESTABLISHING CYBERSECURITY CONTROLS INTO MEDICAL DEVICES

Infosys®
Navigate your next

Significance of Cybersecurity in Medical Devices

The life sciences sector is undergoing a great transformation with the advent of digital technologies. Ever since the organizations, hospitals, and patients switched to low contact, virtual/remote software and devices for tracking, diagnosis, treatment, data management, and other activities the cyber exploitations have increased. The disruptions have impacted patient care. There is a humongous growth in the Internet of Medical Things (IoMT) and connected devices. Although this paradigm shift has improved the patient experience and efficiency of business, it has also brought the risk of security and privacy associated with it. Hence, building a solid foundation to secure the connected devices is the need of the hour. An increase in number of cybersecurity attacks has made medical device companies develop a strong cybersecurity framework at a governance and implementation level.

Key Business Challenges of Cybersecurity in Medical Devices

- Legacy Devices/End of Life
    - Devices that are not supported by vendors would have an outdated Application software or Operating system which might not be compatible with the latest infrastructure of the company. Any cyberattack on the outdated software would pose a risk of compromising the security of the entire network.
- Vulnerability Management
    - Establishing a mechanism to detect the vulnerabilities in medical devices and managing them throughout their life cycle is a key challenge.
- Insufficient Due Diligence of OTS Components
    - Sometimes medical devices may have to incorporate Off The Shelf (OTS) components to meet the overall intended use of the device. Lack of proper impact analysis on the existing issues of these components would lead to security flaws of the medical device.

Hence, the key aspect is to minimize the impact of the above challenges on medical devices. This would need to be done through implementation of mitigating controls (Procedural or Technical). The below sections of the article describe the same in detail.

Cybersecurity in Medical Devices-Industry Guidance

Various Industry regulations/frameworks (Ref Fig 1) formulate the requirements to ensure the cybersecurity of medical devices.

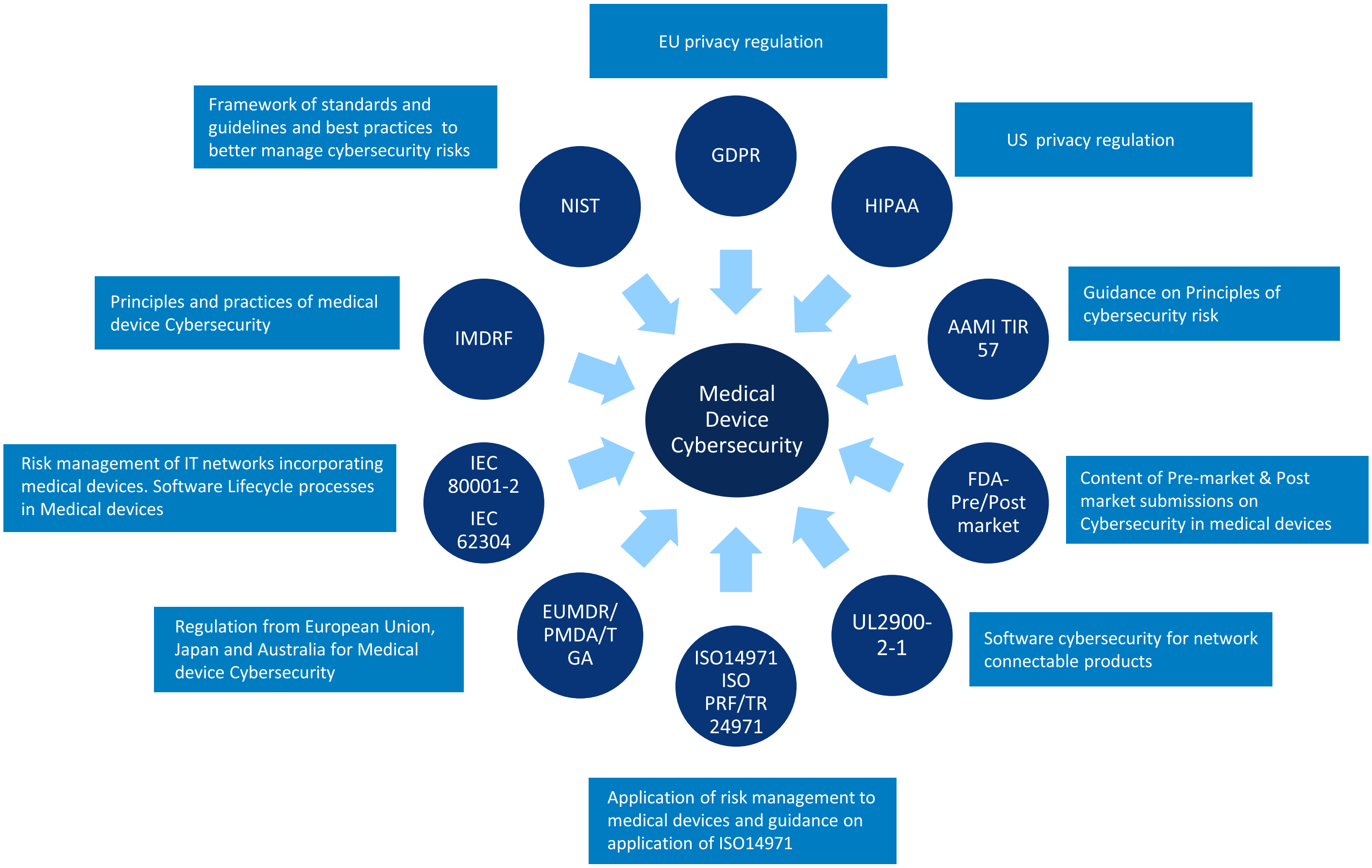

EU privacy regulation
GDPR
Framework of standards and guidelines and best practices to better manage cybersecurity risks
NIST
US privacy regulation
HIPAA
Principles and practices of medical device Cybersecurity
IMDRF
AAMI TIR 57
Guidance on Principles of cybersecurity risk
Medical Device Cybersecurity
Risk management of IT networks incorporating medical devices. Software Lifecycle processes in Medical devices
IEC 80001-2
IEC 62304
FDA-Pre/Post market
Content of Pre-market & Post market submissions on Cybersecurity in medical devices
Regulation from European Union, Japan and Australia for Medical device Cybersecurity
EUMDR/PMDA/TGA
ISO14971 ISO PRF/TR 24971
UL2900-2-1
Software cybersecurity for network connectable products
Application of risk management to medical devices and guidance on application of ISO14971

Fig 1. Industry wide cybersecurity guidelines/regulations

Recommendations from regulatory authorities like FDA/EU MDR revolves around the concept of "Privacy by Design" or "Security by Design," which emphasizes on establishing security controls right from initial phase of medical device development so that these controls are more robust.

The **"NIST"** framework serves as a library of cybersecurity best practices which enables effective management of cybersecurity in medical devices.

The controls should be implemented and validated at each phase of development. Having a structured process of risk assessment is essential to ensure consistency in risk management.

The risk assessment should consider threats posed to all the parties involved. Typically, these would be the key stakeholders like patient, health care professionals, health care facilities, and maintenance personnel. Controls should be designed and established into the device or to the network to ensure mitigation of identified risks. Increased usage of devices might lead to introduction of new sources of threats which need to be identified and controlled as part of continuous risk management.

The below sections explore recommendations from two major regulations, namely FDA & EU MDR

FDA Guidance - Prior to Launch of Medical Devices into the Market

The FDA would need evidence in the form of documentation from device manufacturers on the below when they seek approval to release a device into the market. The FDA insists on using a secure product development process to alleviate the cybersecurity risks associated with medical devices, thus providing reasonable assurance on safety and effectiveness. The below snapshot summarizes the key requirements of the guidance.

Secure Product Development

Security Risk Management

Cybersecurity Risk Assessment

- User threat modeling to assess security risks and design controls
- Details of methods used to transfer security risks into safety risks analysis

Interoperability Considerations

Security controls to ensure Safe and effective exchange of information with another device

Third-Party Software Risks

- Establish SBOM for SOUP or COTS components used in medical devices
- Supporting documentation for SBOM

Residual Risk Analysis

- Publish list of software anomalies in product
- Assess impact on safety and effectiveness of medical devices

Security Architecture

Security Controls

- Built in security controls to device
- Device design procedures to incorporate security features

Architecture Views

- Global system view, multi-patient harm view, patchability view, security use case view
- Establish procedures to implement CAPA
- Demonstrates effectiveness of cybersecurity controls
- Trace architecture views to medical device security requirements

Cybersecurity Testing

Security Requirements

Trace design input requirement to security test case

Vulnerability Testing

Robustness, fuzz testing, static and dynamic code analysis

Penetration Testing

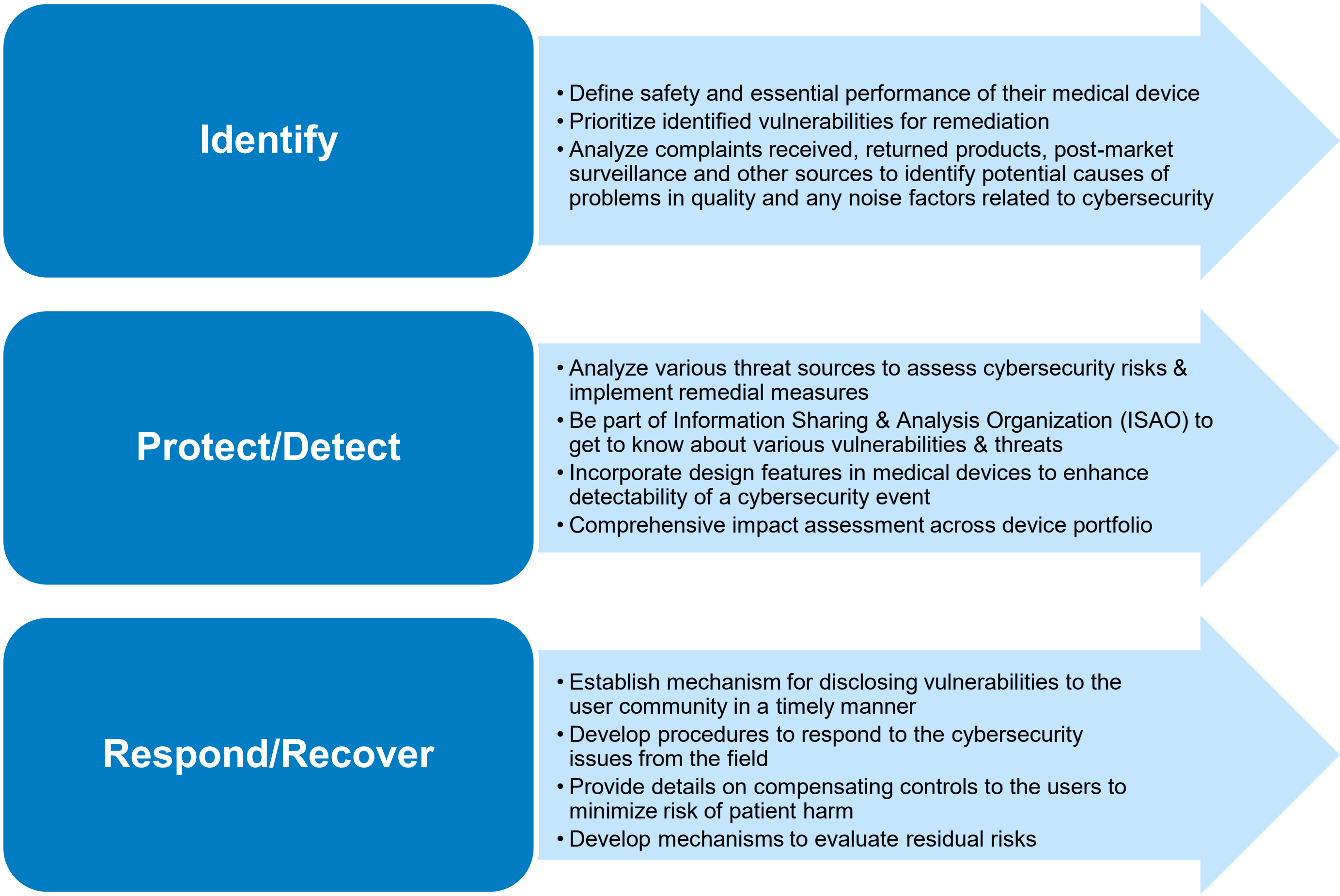
- Independent testing to exploit identified vulnerabilities
- Justification for deferring remediation of identified issues

Apart from the above, labeling considerations is a key step in establishing transparency from the medical device manufacturer in conveying the cybersecurity state of their device to the users.

FDA Guidance - During Deployment of Medical Devices into the Market

Cybersecurity risks are ever evolving. Mitigating all probable cybersecurity risks prior to the deployment of a device into the market is highly difficult. Hence, having a robust process of managing cybersecurity risks post deployment of device to the market is also vital.

Key aspects of an effective post-market cybersecurity management program are as shown below.



Identify

- Define safety and essential performance of their medical device
- Prioritize identified vulnerabilities for remediation
- Analyze complaints received, returned products, post-market surveillance and other sources to identify potential causes of problems in quality and any noise factors related to cybersecurity

Protect/Detect

- Analyze various threat sources to assess cybersecurity risks & implement remedial measures
- Be part of Information Sharing & Analysis Organization (ISAO) to get to know about various vulnerabilities & threats
- Incorporate design features in medical devices to enhance detectability of a cybersecurity event
- Comprehensive impact assessment across device portfolio

Respond/Recover

- Establish mechanism for disclosing vulnerabilities to the user community in a timely manner
- Develop procedures to respond to the cybersecurity issues from the field
- Provide details on compensating controls to the users to minimize risk of patient harm
- Develop mechanisms to evaluate residual risks

EU MDR Guidance

The European Union Medical Device Regulation (EU MDR) prescribes eight key best practices to ensure the cybersecurity of medical devices. A snapshot of the same is depicted below.

Maintain User Documentation

Develop procedures to guide users on steps to configure/update to keep the security intact in medical devices.

Security Update Management

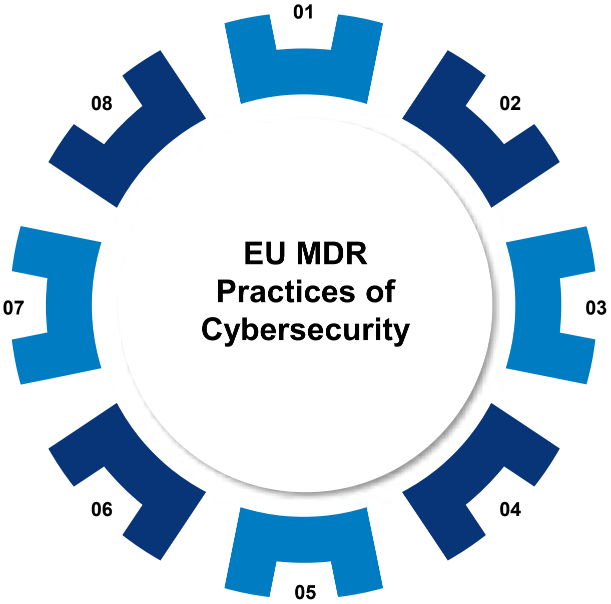
Establish processes to ensure security updates/patches related to medical devices are tested adequately and available on time to users.

Manage Security Issues

Robust processes in place to identify, analyze, and address security related issues on medical devices.

Verification & Validation

Ensure adequate testing of implemented security features at various stages to align with the intended use of device.



EU MDR Practices of Cybersecurity

Plan for Security

Cybersecuirty activities need to be an integral part of medical device product development. The device manufacturer owns responsibility for cybersecurity of third-party components as well.

Security Requirements

Identify security capabilities to meet the security objectives. Few examples are autehtication, encryption, Network segregation, auditing, etc.

Security by Design

Design medical devices to incorporate security requirements. Architecture should reflect the security aspects of medical devices.

Implementation

The design output of medical devices should ensure implementation of security requirements.

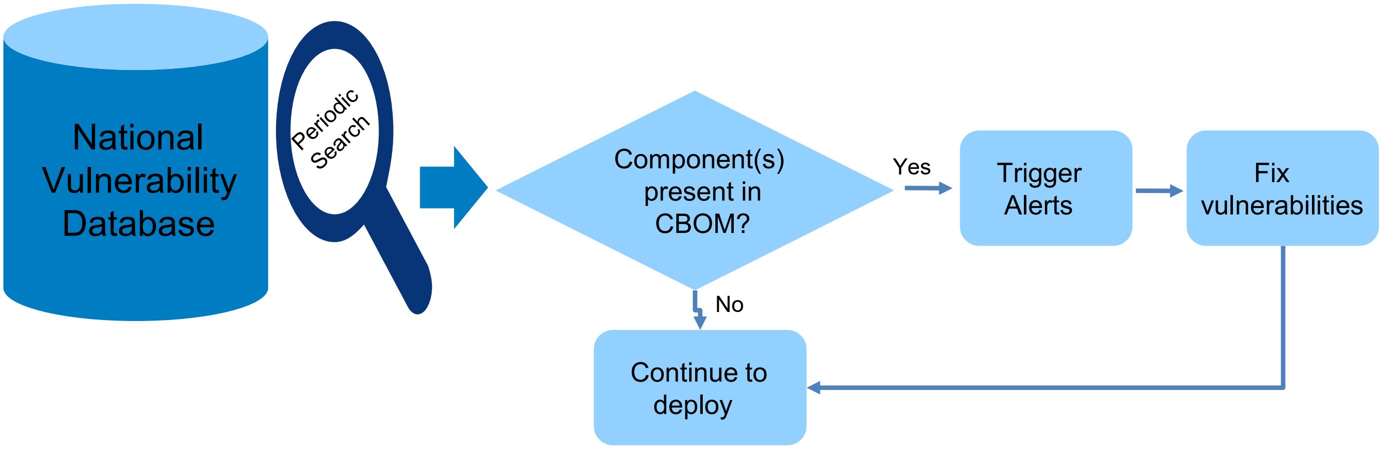
Exploitability of vulnerability is another key factor which determines optimization of effort for risk management activities. Since patient safety is of utmost importance in a medical device, any harm caused to the patient due to exploitation of vulnerability in the device is very crucial. The below snapshot shows the categorization of risk against the exploitation of vulnerability.

Degree of Vulnerability Exploit

Patient Harm

	Low	Medium	High
Negligible	Risk under control	Risk under control	Risk not under control
Minor	Risk under control	Risk under partial control	Risk not under control
Serious	Risk under partial control	Risk not under control	Risk not under control
Critical	Risk not under control	Risk not under control	Risk not under control
Catastrophic	Risk not under control	Risk not under control	Risk not under control

Maintaining Cybersecurity Bill of Materials (CBOM) is a crucial step in assessing the impact of any known vulnerabilities. Quickness of vulnerability identification is the key here. As can be seen from the below snapshot, a periodic monitoring of the Vulnerability Database helps in ascertaining any known vulnerabilities related to the components that we use as part of a medical device and thereby alerting the manufacturer to initiate actions quickly.



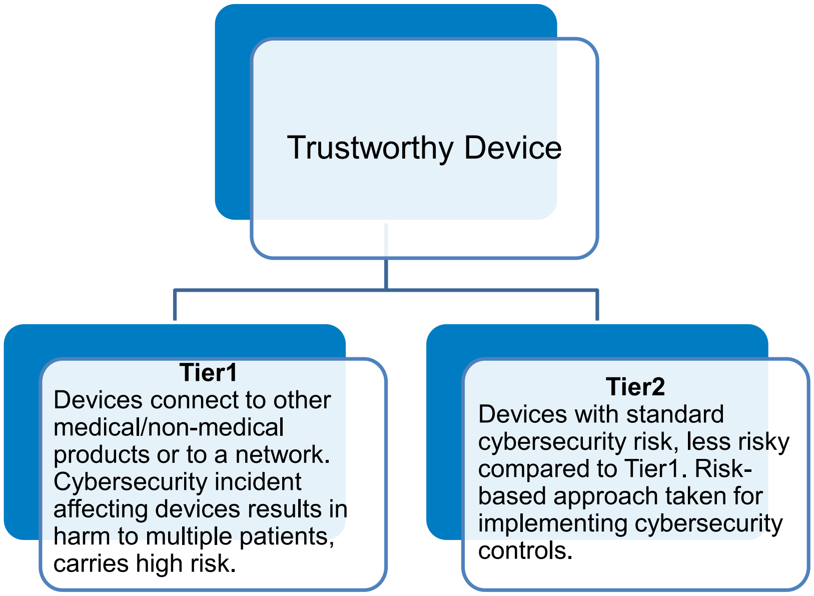
Device manufacturers should diligently publish the vulnerability assessment reports to users. The device users should be informed about the residual risks and current mitigations in place, which enables them to initiate required actions.

Below is a sample of key information that can be captured as part of CBOM

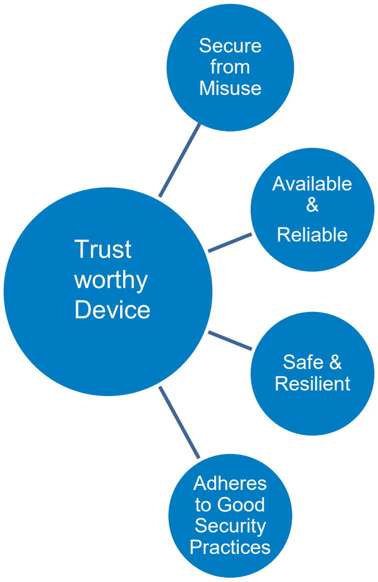
MD product name	Product version	Software Of Unknown Provenance (SOUP) component name	Purpose	Version	Component hash	Vendor	Responsible for applying updates <MD comp / vendor>	Frequency of updates (Quarterly, Semi annual, annual etc.)	Last updated date	End of life date	User notification mode on latest updateportal/ email

Diligent adherence to the above-mentioned practices results in a "Trustworthy Device" which sustains its safety and effectiveness throughout its life cycle. Also, while designing, utmost importance is given to reduction of risk to patients.

The key characteristics of a Trustworthy Device are as depicted below.



Trustworthy Device
Tier1
Devices connect to other medical/non-medical products or to a network. Cybersecurity incident affecting devices results in harm to multiple patients, carries high risk.
Tier2
Devices with standard cybersecurity risk, less risky compared to Tier1. Risk-based approach taken for implementing cybersecurity controls.



Snapshot of the Key Cybersecurity Controls in Medical Devices

✓ Network Security

- Medical device networks are segregated from corporate network
- Secure gateways are used between internal and external networks
- Strong access controls for network devices shall be present

✓ End point protection

- Infrastructure components supporting medical devices to be scanned for Anti virus/Anti malware regularly
- Access to network equipments are strictly controlled physically and logically

✓ Data Protection

- The medical device design ensures encryption of data at rest
- Connectivity to other medical devices or external systems are encrypted with protocol TLS1.2 and above
- Prevent record and replay commands

✓ Wireless Communication

- Wireless network supporting operations of medical devices to be isolated from corporate network
- Authentication and transmission to be encrypted with minimum of AES WPA2.

✓ Event monitoring

- All events (including sdmin activities) of medical devices are monitored and stored as logs
- Periodically review event logs
- Periodically test proper working of monitoring systems

✓ Audit logging

- All user actions are audit trailed
- Messaging systems should retain log of message transmission(date/time,origin, destination) while message content should not be retained

✓ Backup/Restore

- Medical devices handlng ePHI or PII data needs to be backed up and the backed-up data needs to be encrypted
- Periodic restoration tests to be conducted at least once in 6 months

✓ BCP/DR

- Business impact assessment of sequence of events of failures to be performed
- Establish disaster recovery strategy

✓ Vulnerability scanning

- Periodic Penetration testing of Medical devices
- Frequent vulnerability scanning prior to deployment of device into production

✓ Patch management

- Patches are applied in a timely manner and are restricted to authorized personnely only
- Patches are tested prior to applying the same
- Patches for critical vulnerabilities to be applied within 48 hrs

✓ Security Incident Management

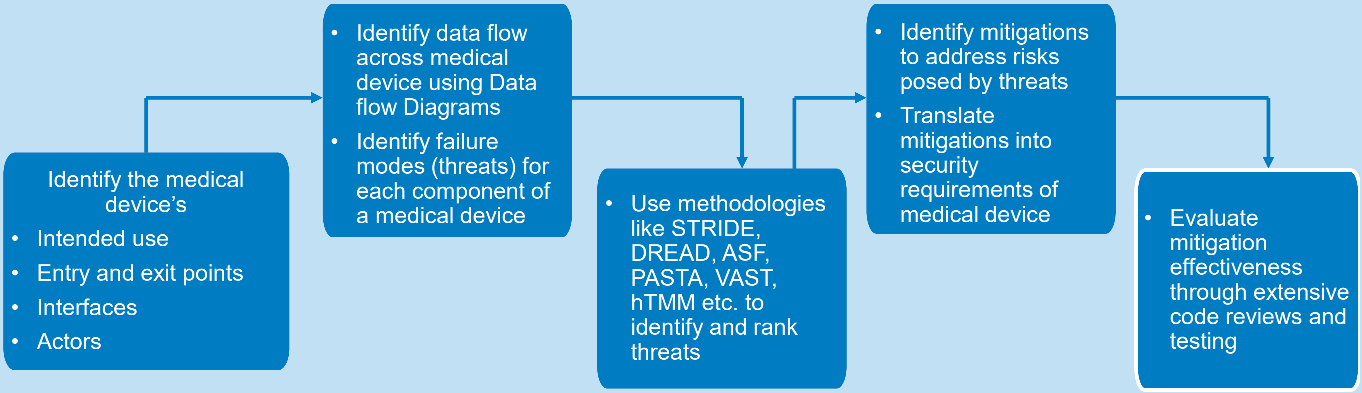
- Defined process to identify, contain, investigate, remedy, and report incidents
- Device to be integrated with SIEM solution to get instant alerts on security incidents

✓ Customer Complaint Handling

- Established process exists for handling queries/complaints for customers
- Hotline for handling emergency issues

Threat Modeling, a Framework for Cybersecurity Risk Assessment

Threat modeling is an activity to identify security and privacy shortcomings of a medical device by analyzing the overall architecture, Flow of data, system boundaries and various failure modes. It also helps in quantifying risks and coming up with actions to mitigate the threats. Threat modeling gives us a point of view of the cybersecurity posture of a medical device from the perspective of an external attack. It is a continuous process, performed throughout the medical device development life cycle. It serves as a solid foundation for improving cybersecurity resilience. Below is the depiction of a typical threat modeling process.



Identify the medical device's
- Intended use
- Entry and exit points
- Interfaces
- Actors

- Identify data flow across medical device using Data flow Diagrams
- Identify failure modes (threats) for each component of a medical device

- Use methodologies like STRIDE, DREAD, ASF, PASTA, VAST, hTMM etc. to identify and rank threats

- Identify mitigations to address risks posed by threats
- Translate mitigations into security requirements of medical device

- Evaluate mitigation effectiveness through extensive code reviews and testing

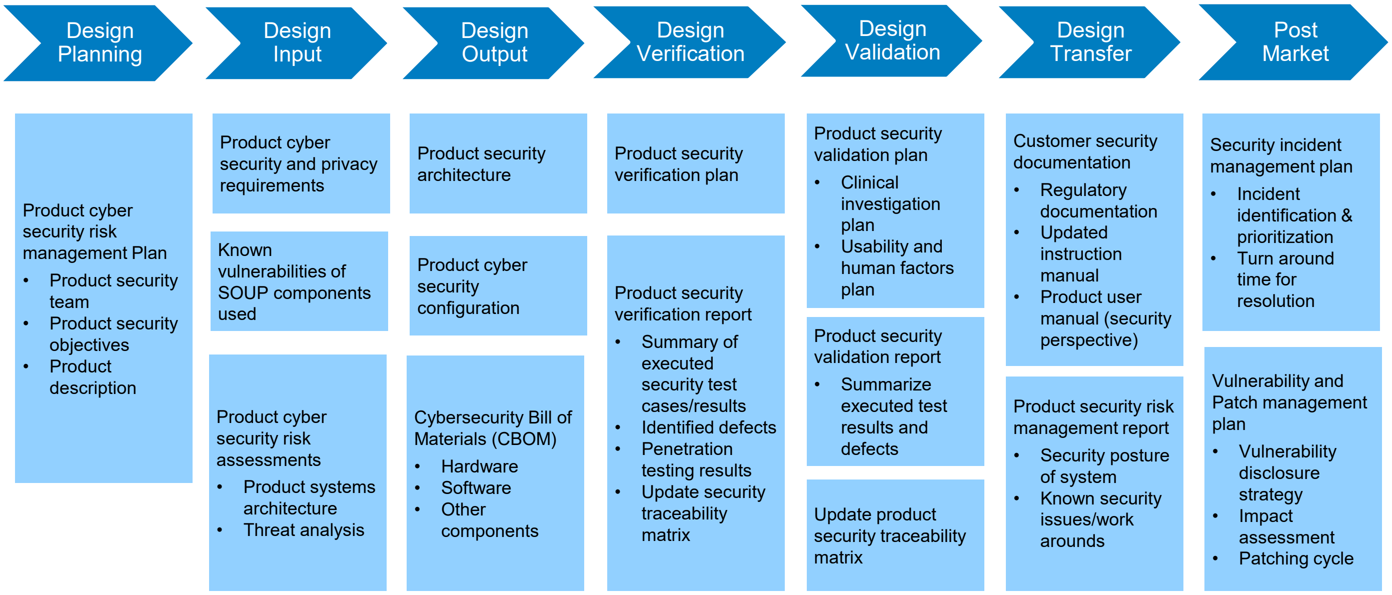
STRIDE→ Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
DREAD → Damage, Reproducibility, Exploitability, Affected Users, Discoverability
ASF → Application Security Frame (Categorizes threats into areas of weaknesses like auditing, authentication, data protection
PASTA → Process for Attack Simulation and Threat Analysis
VAST → Visual, Agile, and Simple Threat
hTMM → hybrid Threat Modeling Method

Microsoft Threat Modeling tool and OWASP Threat Dragon are some of the tools which can be used to perform threat modeling.

Cybersecurity DHF Deliverables across the Life Cycle

Design History File (DHF) is the compilation of all design control documents developed across the development life cycle of a Medical Device. These artifacts would be essential during Regulatory submission towards getting the Medical Device approval for its intended use.

Below diagram depicts various DHF deliverables that are published from the perspective of Cybersecurity during the Secure Software Development Life Cycle of Medical Device.



Design Planning

Product cyber security risk management Plan
- Product security team
- Product security objectives
- Product description

Design Input

Product cyber security and privacy requirements

Known vulnerabilities of SOUP components used

Product cyber security risk assessments
- Product systems architecture
- Threat analysis

Design Output

Product security architecture

Product cyber security configuration

Cybersecurity Bill of Materials (CBOM)
- Hardware
- Software
- Other components

Design Verification

Product security verification plan

Product security verification report
- Summary of executed security test cases/results
- Identified defects
- Penetration testing results
- Update security traceability matrix

Design Validation

Product security validation plan
- Clinical investigation plan
- Usability and human factors plan

Product security validation report
- Summarize executed test results and defects

Update product security traceability matrix

Design Transfer

Customer security documentation
- Regulatory documentation
- Updated instruction manual
- Product user manual (security perspective)

Product security risk management report
- Security posture of system
- Known security issues/work arounds

Post Market

Security incident management plan
- Incident identification & prioritization
- Turn around time for resolution

Vulnerability and Patch management plan
- Vulnerability disclosure strategy
- Impact assessment
- Patching cycle

Final Thoughts

Cybersecurity has a vast scope in the medical device industry. With the advent of new age digital technologies and increased connectivity, building cybersecurity controls right in the first place is the key rather than expending effort in testing for presence of any vulnerabilities and fixing them.

The need for having a dedicated cybersecurity team to identify, design, implement, and test cybersecurity requirements is of prime importance to mitigate the risk of patient harm. It is an area where the medical device manufacturers should invest and make sure to understand the requirements as per the standards/regulations and then build those cybersecurity controls into the device which is very crucial in ensuring patient safety.

References

1. Software as Medical Device Market Size & Growth Analysis Report (bccresearch.com)

2. FDA Premarket and Post-market Cybersecurity Guidelines

3. NIST Framework-https://www.nist.gov

4. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

5. New Cybersecurity Requirements for EU MDR

Authors

Kumar Nagesh

Senior consultant-Infosys consulting

Kumar works with Life sciences consulting. He has 15 years of experience in the field of Governance Risk & compliance encompassing the areas of computer system validation, Medical Devices, Security controls assessment and vendor risk management.

Ashrith Karru

Senior Consultant-Infosys Consulting

Ashrith is in life science practice, supporting governance, risk and compliance. He has 17 years of industry experience in information security, quality management systems, process definition, product development life cycle methodologies, and standard. He is experienced in implementation of NIST framework, cloud control matrix, HIPAA, ISO 27001, ISO 13485, six sigma, agile and CMMI.

For more information, contact askus@infosys.com

Infosys®
Navigate your next